FIFO ARCHITECTURE WITH IN-PLACE CRYPTOGRAPHIC SERVICE

Background of the Invention

1. Field of the Invention

This invention relates generally to encryption/decryption techniques, and more particularly to a FIFO architecture with in-place cryptographic service.

2. Description of the Prior Art

Known encryption/decryption techniques typically require multiple rounds (or stages) to complete, causing latency, typically as many as 16 clock cycles. When processing real time packet transmissions/reception, this latency must be accommodated by buffers, otherwise the cryptographic service must run at up to sixteen times the data transmission clock frequency.

In view of the foregoing, it is desirable to provide a method and structure for providing cryptographic service that does not require additional buffers or difficult buffer size decisions to compensate for latency and that is not required to run faster than the data transmission clock frequency.

Summary of the Invention

The present invention is directed to a FIFO that is implemented as a buffer to encrypt/decrypt packet data and return the data to the same location where it was initially stored. No additional buffer or difficult buffer size decision is therefore required to compensate for the latency associated with the encryption/decryption. The FIFO implementation includes primary and secondary pointers. The primary pointers are available to the transmit/receive circuitry and the secondary pointers are used by the cryptographic circuit. When data is initially loaded into the FIFO, the FIFO does not report data availability to the primary user until the secondary user (cryptographic service) has read a block and returned the block to the same location. The FIFO is implemented via a single port RAM. Blocks are based on the encryption block size. The FIFO similarly reports packet availability based on application packet sizes (such as 188 MPEG2 transport stream packets).

According to one aspect of the invention, a FIFO is implemented as a buffer to encrypt/decrypt packet data and return the data to the same location where it was initially stored eliminating the need for a dedicated cryptographic service (latency) buffer for storing received data.

According to another aspect of the invention, a FIFO is implemented as a buffer to encrypt/decrypt packet data and return the data to the same location where it was initially stored to provide an encryption/decryption engine that can run with slower clock speeds than that required using known encryption/decryption engines.

According to yet another aspect of the invention, a FIFO is implemented as a buffer to encrypt/decrypt packet data and return the data to the same location during the time between packets, effectively smoothing the timeline.

According to still another aspect of the invention, a FIFO is implemented as a buffer to encrypt/decrypt packet data and return the data to the same location using reduced clock frequency requirements on the cryptographic engine, saving power and logic gates.

According to still another aspect of the invention, a FIFO is implemented as a buffer to encrypt/decrypt packet data and return the data to the same location using a

flexible configuration that allows packet parsing or filtering in combination with the cryptographic service.

According to still another aspect of the invention, a FIFO is implemented as a buffer to encrypt/decrypt packet data and return the data to the same location using only a single port RAM.

According to still another aspect of the invention, a FIFO is implemented as a buffer to encrypt/decrypt packet data and return the data to the same location in which the adaptation fields and various other fields are not scrambled, while the payload field is scrambled.

Brief Description of the Drawings

Other aspects, features and advantages of the present invention will be readily appreciated as the invention becomes better understood by reference to the following detailed description when considered in connection with the accompanying drawing figure wherein:

Figure 1 is a block diagram illustrating a well known technique using encryption/decryption service after a FIFO;

Figure 2 is a block diagram illustrating a well known technique using encryption/decryption service before a FIFO;

Figure 3 is a block diagram illustrating encryption/decryption service that resides as a part of a FIFO system according to one embodiment of the present invention;

Figure 4 is a diagram illustrating addressing and data storage associated with the FIFO system shown in Figure 3; and

Figure 5 is a block diagram illustrating a more complex FIFO architecture that employs a switcher and a single encryption algorithm that resides as a part of the FIFO architecture to accommodate converting encrypted data associated with two paths according to another embodiment of the present invention.

While the above-identified drawing figures set forth particular embodiments, other embodiments of the present invention are also contemplated, as noted in the discussion. In all cases, this disclosure presents illustrated embodiments of the present invention by way of representation and not limitation. Numerous other modifications and embodiments can be devised by those skilled in the art which fall within the scope and spirit of the principles of this invention.

Detailed Description of the Preferred Embodiments

The present invention is best understood by first describing known techniques illustrated herein below with reference to Figures 1 and 2 for providing encryption/decryption service in association with a FIFO.

Figures 1a and 1b are block diagrams illustrating a well known technique using encryption/decryption service after a FIFO 10. As shown in Figure 1a, received packets are decrypted by reading out the data from the FIFO 10 through a decryption service 12. Transmitting packets are encrypted by writing the packets in to the FIFO 10 through an encryption service 14 as shown in Figure 1b. This technique is advantageous since a large buffer is unnecessary. This technique is disadvantageous however, since the speed of the associated encryption/decryption circuit 12, 14 is governed by the I/F speed. Further, special care must be taken when dealing with the FIFO 10 whenever the encryption/decryption content key has changed during the operation, another disadvantage. Yet another disadvantage is associated with the case of packet transmission, in which write operations must take place through encryption logic that requires constant awareness of the encryption logic.

Figures 2a and 2b are block diagrams illustrating a well known technique using encryption/decryption service before a FIFO 10. As shown in Figure 2a, received packets are decrypted on-the-fly and stored into FIFO 10. Transmitting packets shown in Figure 2b are stored in the FIFO 10 in the form of unencrypted data and are encrypted in the background. This technique is advantageous in that the data in the FIFO 10 is always unencrypted data. In this regard, the encryption/decryption service is transparent to the user. This technique is, however, disadvantageous in that a large buffer 20 is required to fill the speed difference between the packet speed and the encryption/decryption logic speed. Further, a high speed clock may be necessary to run the encryption/decryption logic associated with decryption service 12 and encryption service 14.

Figure 3 is a block diagram illustrating encryption/decryption service 32 that resides as a part of a FIFO system 30 according to one embodiment of the present invention. Received packets are first stored into a FIFO 34, then read out by encryption circuitry associated with encryption/decryption service 32 where it is written back into

the FIFO 34. Those skilled in the art will readily appreciate that transmitting packets works in substantially the same manner. The encryption/decryption service 32 is not visible to the user, but instead, appears to the user as nothing more than a simple FIFO. No dedicated buffer is necessary to compensate for speed differences since all encryption/decryption takes place inside the FIFO 34. Since the encryption/decryption service 32 is internal only to the FIFO 34, the speed of encryption/decryption is not governed by any physical clock speed; and the encrypted data is more secure when compared with that associated with known encryption/decryption engines.

Figure 4 is a diagram illustrating addressing and data storage associated with the FIFO system 30 shown in Figure 3. The FIFO 34 can be seen to have four address pointers. The first address pointer 36 is associated with a primary write address that specifies the address written to the FIFO 34. The second address pointer 38 is associated with a primary read address that specifies the address where a user reads out data from the FIFO 34. The third address pointer 40 is associated with a secondary read address that specifies the address read by the encryption/decryption service 32. The fourth address pointer 42 is associated with a secondary write address that specifies where the processed data is written back into the FIFO 34. The data 44 between the secondary write address and the primary read address is available for a user.

Figure 5 is a block diagram illustrating a more complex FIFO architecture 50 that employs a switcher 52 and a single encryption algorithm that resides as a part of the FIFO architecture 50 to accommodate converting encrypted data associated with two paths according to another embodiment of the present invention. The encryption/decryption service 32 works in the same manner as described herein before with reference to Figures 3 and 4, except that now a switcher 52 is used to multiplex the encryption/decryption service 32 between two different FIFO devices 54, 56 such that data can now be processed in a time sharing manner to accommodate two distinct data paths.

In view of the above, it can be seen the present invention presents a significant advancement in the art of encryption/decryption techniques. Further, this invention has been described in considerable detail in order to provide those skilled in the encryption/decryption art with the information needed to apply the novel principles and to construct and use such specialized components as are required. In view of the

foregoing descriptions, it should be apparent that the present invention represents a significant departure from the prior art in construction and operation. However, while particular embodiments of the present invention have been described herein in detail, it is to be understood that various alterations, modifications and substitutions can be made therein without departing in any way from the spirit and scope of the present invention, as defined in the claims which follow.